



Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

Arithmetical Theory of Certain Hurwitzian Continued Fractions.

BY D. N. LEHMER.

Introduction.

The following investigation is the outcome of the discovery, made some three years ago, of the curious fact that the denominator of the convergent of order $3n$ in the regular continued fraction which represents the base of Napierian logarithms is divisible by n . It was later found that the same is true of the denominators of the convergents of order $3n-2$ and $3n-6$, and of the numerator of the convergent of order $3n-3$. Further, the convergents were found to recur with a period of $3n$ terms, or of $6n$ terms according as n is even or odd.

These theorems, discovered empirically, turned out to be remarkably intractable, and, although, a year ago, a method was discovered of establishing them, it would not apply to other continued fractions of the same general type for which the same or similar theorems seemed to hold.

The discovery of the regular continued fraction

$$e = (2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, \dots),$$

for the base of Napierian logarithms is credited to Roger Cotes,* but to Euler† is due the rediscovery of it, and the general proof of the law of the successive partial quotients by means of the solution of Riccati's equation. Euler also found other remarkable continued fractions such as

$$\begin{aligned} e &= (1, 1, 1, 1, 5, 1, 1, 9, 1, 1, 14, 1, 1, \dots), \\ (e^{\frac{1}{s}} + 1)/(e^{\frac{1}{s}} - 1) &= (2s, 6s, 10s, 14s, \dots), \\ e^{\frac{1}{s}} &= (1, s-1, 1, 1, 3s-1, 1, 1, 5s-1, 1, 1, \dots). \end{aligned}$$

Hurwitz‡ has studied a very general type of continued fraction, to which the above fractions all belong. He makes use of the notation

$$(q_1, q_2, \dots, q_r, \overline{f_1(m), f_2(m), f_3(m), \dots, f_k(m)}), \quad (m=0, 1, 2, 3, \dots),$$

for the continued fraction whose partial quotients are

$$\begin{aligned} q_1, q_2, \dots, q_r, f_1(0), f_2(0), \dots, f_k(0), f_1(1), f_2(1), \dots, f_k(1), \\ f_1(2), f_2(2), \dots, \end{aligned}$$

* Cotes, "Logometria," *Phil. Trans.*, London (1714), Vol. XXIX, p. 5.

† Euler, *Comm. Acad. Petrop.* (1737), p. 121, edition of 1744.

‡ Hurwitz, *Vierteljahrsschrift der Naturforschenden Gesellschaft in Zurich* (1896), Vol. XLI, p. 34.

where the q 's are rational, and with the possible exception of q_1 , all positive. The functions f are rational, integral functions whose degrees may some or all be zero. If, however, the degrees are all zero, the fraction becomes an ordinary periodic continued fraction. If the highest degree found among any of the functions is m , the fraction is said to be of the m -th order. An ordinary periodic continued fraction is thus a Hurwitzian fraction of order zero. Written in this notation the above fractions of Euler read:

$$\begin{aligned} e &= (2, \overline{1, 2m+2, 1}), & (m=0, 1, 2, 3, \dots), \\ (e^{\frac{1}{s}}+1)/(e^{\frac{1}{s}}-1) &= [(4m+2)s], & (m=0, 1, 2, 3, \dots), \\ e^{\frac{1}{s}} &= [1, \overline{(2m+1)s, 1}], & (m=0, 1, 2, 3, \dots), \end{aligned}$$

Hurwitz has shown that if the irrational numbers ξ and η are connected by the equation $\xi = (\alpha\eta + \beta)/(\gamma\eta + \delta)$, where $\alpha, \beta, \gamma, \delta$ are integers such that $\alpha\delta - \beta\gamma$ is not zero, then if the regular continued fraction for η is of the Hurwitzian type, so also is that for ξ , and the functions f appearing in each expansion are of the same degrees, with the possible exception of those of zero degree which may appear in one and not in the other.

In this paper we shall deal with Hurwitzian fractions in which the functions f are all of degree zero except one, and that one is of the first degree. We shall write the fraction in the form:

$$(q_1, q_2, \dots, q_r, \overline{a_1, a_2, a_3, \dots, a_{k-1}, bm+c}), \quad (m=1, 2, 3, \dots),$$

and taking first the case where the q 's are all absent, we show that, with certain interesting exceptions, it is true for all such fractions that the numerator of the convergent of order $2nk-1$, and the denominator of the convergent of order $2nk$ are divisible by n , while the numerator of the convergent of order $2nk$, and the denominator of the convergent of order $2nk-1$ are congruent modulo n to $(-1)^{nk-1}$, so that the series of convergents repeat themselves, modulo n after $4nk$ terms, or after $2nk$ terms according as nk is even or odd.

Exceptions to this rule occur when b is congruent to zero, modulo n , or when the numerator or denominator of the convergent of order $k-1$ is congruent to zero, modulo n . The period of the convergents is not so simply stated for these cases.

The laws for the period of the fraction when the q 's are actually present are easily obtainable.

In this paper we are not considering questions of convergence or divergence of continued fractions. Certain of the fractions involved are closely related to those called "semiregular" whose convergence has been studied by

Tietze,* and the rules for determining convergence or divergence of semi-regular continued fractions may be modified to apply to them. We are concerned here with the successive values of the numerators and denominators of the convergents, and not with the existence or non-existence of a limiting value to those convergents. The theorems obtained have to do with numbers which satisfy certain difference equations of the second order, and are thus, as Professor Birkhoff has remarked, extensions of Wilson's and Fermat's theorems, which have to do with numbers which satisfy the difference equations $u_{n+1}=nu_n$ and $u_{n+1}=au_n$ respectively.

I.

Let A_m/B_m be the m -th convergent of the continued fraction

$$(\overline{a_1, a_2, a_3, \dots, a_{k-1}, \mu b}), \quad (\mu=1, 2, 3, \dots), \quad (1)$$

where all the partial quotients are positive or negative integers or zero. Let also A'_m/B'_m be the m -th convergent of the fraction

$$(\overline{a_{k-1}, a_{k-2}, \dots, a_2, a_1, -b\mu-2M}), \quad (\mu=1, 2, \dots), \quad (2)$$

where

$$M=(A_{k-2}+B_{k-1})/A_{k-1}, \quad (3)$$

and we will suppose that A_{k-1} is not zero. We will show by complete induction that the following equations hold:

$$A_{rk-1}=A'_{rk-1}(-1)^{r-1}, \quad (4)$$

$$A_{rk}=(A'_{rk}+MA'_{rk-1})(-1)^r. \quad (5)$$

By using equation (4) we may interchange A and A' in (5).

To start the proof it is necessary to show that the formulae hold for $r=1$. The fractions $(a_1, a_2, a_3, \dots, a_{k-1})$ and $(a_{k-1}, \dots, a_2, a_1)$ are inverse. (See Perron, "Die Lehre von den Kettenbrüchen," p. 32). We have, therefore, $A'_{k-1}/A'_{k-2}=(a_1, a_2, \dots, a_{k-1})=A_{k-1}/B_{k-1}$, and since the fractions are in their lowest terms,

$$A_{k-1}=A'_{k-1}, \quad (6)$$

$$B_{k-1}=A'_{k-2}; \quad (7)$$

and similarly,

$$A_{k-2}=B'_{k-1}, \quad (8)$$

$$B_{k-2}=B'_{k-2}. \quad (9)$$

Equation (4) therefore holds when $r=1$, by (6). Also, from the definition of M we have, using (6) again, $MA'_{k-1}=A_{k-2}+B_{k-1}$, so that when $r=1$, (5) becomes

$$A_k=-(A'_k+A_{k-2}+B_{k-1}). \quad (10)$$

*Tietze, *Math. Ann.* (1911), Vol. LXX.

But from the definitions of the continued fractions themselves we have

$$A_k = bA_{k-1} + A_{k-2}, \quad (11)$$

and
$$A'_k = -(b + 2M)A'_{k-1} + A'_{k-2}; \quad (12)$$

or, using (6) and (7),

$$A'_k = -(bA_{k-1} + 2A_{k-2} + B_{k-1}). \quad (13)$$

Substituting (11) and (13) in (10) it is found that equation (5) is true when $r=1$.

We now show that if equations (4) and (5) are assumed to hold for all values of r up to and including $r=n$, they must also hold for $r=n+1$.

By the fundamental formula of continued fractions (see Perron, *loc. cit.*, p. 14),

$$A_{(n+1)k-1} = A_{k-1}A_{nk} + B_{k-1}A_{nk-1}, \quad (14)$$

and assuming formulae (4) and (5) for $r=n$ this gives

$$A_{(n+1)k-1} = (-1)^n A_{k-1} (A'_{nk} + MA'_{nk-1}) + (-1)^{n-1} A'_{nk-1} B_{k-1},$$

and, recalling the definition of M , this becomes

$$A_{(n+1)k-1} = (-1)^n (A_{k-1}A'_{nk} + A_{k-2}A'_{nk-1}),$$

and using (6) and (8) this is $A_{(n+1)k-1} = (-1)^n (A'_{k-1}A'_{nk} + B'_{k-1}A'_{nk-1})$, which, by the fundamental formula (14), gives

$$A_{(n+1)k-1} = (-1)^n A'_{(n+1)k-1}, \quad (15)$$

which is formula (4) for $r=n+1$.

Suppose now that formula (5) holds for $r=n$, so that

$$A_{nk} = (-1)^n (A'_{nk} + MA'_{nk-1}).$$

Multiply both sides of this equation by A_{k-2} , and add $B_{k-2}A_{nk-1}$ to the left-hand side, and the equal expression, $(-1)^{n-1}B_{k-2}A'_{nk-1}$ to the right. We thus obtain

$$A_{k-2}A_{nk} + B_{k-2}A_{nk-1} = (-1)^n (A_{k-2}A'_{nk} + MA_{k-2}A'_{nk-1} - B_{k-2}A'_{nk-1}).$$

Using (6), (7), (8) and (9), we can throw this into the form

$$A_{k-2}A_{nk} + B_{k-2}A_{nk-1} = (-1)^n [M(A'_{k-1}A'_{nk} + B'_{k-1}A'_{nk-1}) - (A'_{k-2}A'_{nk} + B'_{k-2}A'_{nk-1})].$$

But by the fundamental formulae of continued fractions (Perron, *loc. cit.*, p. 14), this last equation may be written $A_{(n+1)k-2} = (-1)^n (MA'_{(n+1)k-1} - A'_{(n+1)k-2})$. To the left side of this equation add the term $(n+1)bA_{(n+1)k-1}$, and to the right side add the term $(-1)^n(n+1)bA'_{(n+1)k-1}$, which by equation (15) is legitimate, and the result is

$$\begin{aligned} (n+1)bA_{(n+1)k-1} + A_{(n+1)k-2} \\ = (-1)^{n+1} [-(n+1)bA'_{(n+1)k-1} - MA'_{(n+1)k-1} + A'_{(n+1)k-2}]. \end{aligned} \quad (16)$$

But from the recurrent relation connecting the numerators in the continued fraction we have $A_{(n+1)k} = (n+1)A_{(n+1)k-2} + A_{(n+1)k-1}$, and

$$A'_{(n+1)k} = -[(n+1)b + 2M]A'_{(n+1)k-1} + A'_{(n+1)k-2}.$$

Putting these values in (16) we get $A_{(n+1)k} = (-1)^{n+1}(A'_{(n+1)k} + MA'_{(n+1)k-1})$, which is equation (5) when $r = n+1$. If then (4) and (5) are true for $r = n$, they must be true for $r = n+1$. But they have been shown to hold for $r = 1$, therefore they hold in general.

II.

Consider now the continued fraction

$$(x, a_{k-1}, a_{k-2}, \dots, a_2, a_1, y, \overline{a_{k-1}, a_{k-2}, \dots, a_2, a_1, -b\mu - 2M}),$$

$$(\mu = 1, 2, \dots), \quad (17)$$

where

$$x = (B_{k-1} - A_{k-2})/A_{k-1}, \quad (18)$$

and

$$y = -(2B_{k-1}^2 + A_{k-1}B_k + A_{k-1}B_{k-2})/A_{k-1}B_{k-1}. \quad (19)$$

We assume that A_{k-1} and B_{k-1} are different from zero. We denote the $(m+1)$ st convergent of this fraction by A''_m/B''_m , and show by complete induction that the following equations hold:

$$B_{rk-1} = A''_{rk-1}(-1)^{r-1}, \quad (20)$$

$$B_{rk} = (A''_{rk} + MA''_{rk-1})(-1)^r. \quad (21)$$

Equation (21) may be written, using (20),

$$A''_{rk} = (B_{rk} + MB_{rk-1})(-1)^r. \quad (22)$$

We first show that the formulae hold when $r = 1$. We have $A''_{k-1}/B''_{k-1} - x = (0, a_{k-1}, a_{k-2}, \dots, a_1)$, or $B''_{k-1}/(A''_{k-1} - xB''_{k-1}) = (a_{k-1}, \dots, a_1) = A'_{k-1}/B'_{k-1} = A_{k-1}/A_{k-2}$, and since all fractions are in their lowest terms,

$$B''_{k-1} = A_{k-1}, \quad (23)$$

$$A''_{k-1} - xB''_{k-1} = A_{k-2}. \quad (24)$$

From these two equations with (18) we get at once

$$A''_{k-1} = B_{k-1}, \quad (25)$$

which is formula (20) when $r = 1$.

In the same way, using the relations $B''_{k-2}/(A''_{k-2} - xB''_{k-2}) = (a_{k-1}, \dots, a_2) = A'_{k-2}/B'_{k-2} = B_{k-1}/B_{k-2}$, we get

$$B''_{k-1} = B_{k-1}, \quad (26)$$

$$A''_{k-2} = xB_{k-1} + B_{k-2}, \quad (27)$$

whence, using the defining equation for x again, and remembering from the general theory of continued fractions that

$$A_{k-1}B_{k-2} - B_{k-1}A_{k-2} = (-1)^{k-1}, \quad (28)$$

Equation (27) reduces to

$$A''_{k-2} = [B_{k-1}^2 + (-1)^{k-1}] / A_{k-1}. \quad (29)$$

Now $A''_k = yA''_{k-1} + A''_{k-2}$, and using the defining equation for y together with (25) and (27) we get from this,

$$A''_k = -[B_{k-1}^2 + A_{k-1}(B_k + B_{k-2}) - (-1)^{k-1}] / A_{k-1}. \quad (30)$$

Recall now the definition of M and we get

$$A''_k + MA''_{k-1} = -[B_{k-1}^2 + A_{k-1}(B_k + B_{k-2}) - A_{k-2}B_{k-1} - (-1)^{k-1} - B_{k-1}^2] / A_{k-1},$$

which reduces again, using (28), to

$$A''_k + MA''_{k-1} = -B_k, \quad (31)$$

which agrees with formula (21) when $r=1$.

We now show that if formulae (20) and (21) are true for all values of r up to and including $r=n$ they must hold for $r=n+1$. We have, using again the formulae given in Perron, page 14, $A_{(n+1)k-1} = A_{k-1}A_{nk} + B_{k-1}A_{nk-1}$, and using formulae (20) and (21), which are assumed to hold for $r=n$, this may be written: $A''_{(n+1)k-1} = (-1)^n A_{k-1}(B_{nk} + MB_{nk-1}) + (-1)^{n-1} A_{k-2}B_{nk-1}$. Putting in the value of M we get from this,

$$A''_{(n+1)k-1} = (-1)^n (A_{k-1}B_{nk} + B_{k-1}B_{nk-1}) = (-1)^n B_{(n+1)k-1},$$

which is formula (20) when $r=n+1$.

Starting now with the equation which comes from the way the continued fraction is defined,

$$B_{(n+1)k} = (n+1)bB_{(n+1)k-1} + B_{(n+1)k-2}, \quad (32)$$

we write it, using the fundamental recursion formulae (Perron, p. 14),

$$B_{(n+1)k} = (n+1)bB_{(n+1)k-1} + A_{k-2}B_{nk} + B_{k-2}B_{nk-1}.$$

This may again be written (since $B_{(n+1)k-1} = A_{k-1}B_{nk} + B_{k-1}B_{nk-1}$),

$$B_{(n+1)k} = [(n+1)b + M]B_{(n+1)k-1} - B_{k-1}(B_{nk} + MB_{nk-1}) + B_{k-2}B_{nk-1}, \quad (33)$$

but for $r=n$ we have, by hypothesis, using (22) and (20),

$$B_{nk} + MB_{nk-1} = A''_{nk}(-1)^n, \quad B_{nk-1} = (-1)^{n-1}A''_{nk-1}.$$

Also, by (7) and (9), $B_{k-1} = A'_{k-2}$, $B_{k-2} = B'_{k-2}$. Putting these values in (33) we get

$$B_{(n+1)k} = [(n+1)b + M]B_{(n+1)k-1} + (-1)^{n+1}(A'_{k-2}A''_{nk} + B'_{k-2}A''_{nk-1}), \quad (34)$$

but again, from the construction of the fraction $A''_{(n+1)k-2} = A'_{k-1}A''_{nk} + B'_{k-2}A''_{nk-1}$, and (34) becomes

$$B_{(n+1)k} = [(n+1)b + M]B_{(n+1)k-1} + (-1)^{n+1}A''_{(n+1)k-2}. \quad (35)$$

Now we have already shown that formula (20) holds for $r=n+1$ so that we can write $B_{(n+1)k-1} = (-1)^n A''_{(n+1)k-1}$ in (35), and get

$$B_{(n+1)k} = (-1)^{n+1}[(n+1)b + M]A''_{(n+1)k-1} + A''_{(n+1)k-2}. \quad (36)$$

But again, from the succession of partial quotients of the continued fraction, $A''_{(n+1)k} = -[(n+1)b + 2M]A''_{(n+1)k-1} + A''_{(n+1)k-2}$, ($n=1, 2, 3, \dots$). This in (36) gives $B_{(n+1)k} = (-1)^{n+1}(A''_{(n+1)k} + MA''_{(n+1)k-1})$, which is formula (21) when $r=n+1$. These formulae therefore hold in all cases.

From the definition of M it would seem that k must not be less than 3. With the usual conventions, however, that $A_0=1$, $B_0=0$, $A_{-1}=0$ and $B_{-1}=1$, the theorems derived above will apply when $k=1$ and $k=2$.

III.

We consider now the continued fractions (1), (2) and (17) with respect to any modulus n , and we assume that n is prime to $2b$ and to A_{k-1} and to B_{k-1} . The cases where these restrictions are not applied will be considered later. It is then possible to find two values of μ , one odd and the other even, both less than $2n$, which will satisfy the congruence

$$b\mu + 2M \equiv 0 \pmod{n}. \quad (37)$$

Such a solution will furnish a zero partial quotient in the continued fraction (2) of rank μk , and the partial quotient of the same rank in fraction (1) will have the value $-2M$. Moreover, it is seen that the partial quotients of (2) read backward from this partial quotient exactly as the partial quotients of (1) read forward, so that, taken modulo n , the two fractions are inverse as far as this partial quotient. We consider first the even solution of (37), which we denote by $2m$. By the properties of inverse fractions we have (see equations (6), (7), (8) and (9)) $A_{2mk-1} \equiv A'_{2mk-1} \pmod{n}$. But by equation (4), $A_{2mk-1} = -A'_{2mk-1}$, so that

$$A_{2mk-1} \equiv 0 \pmod{n}. \quad (38)$$

IV.

The partial quotient of rank $2m$ is, as we noted above, congruent to $-2M$, the two preceding ones being a_{k-1} and a_{k-2} . The recursion formulae for a continued fraction give

$$A_{2mk} = -2MA_{2mk-1} + A_{2mk-2}, \quad (39)$$

$$A_{2mk-1} = a_{k-1}A_{2mk-2} + A_{2mk-3}, \quad (40)$$

$$A_{2mk-2} = a_{k-2}A_{2mk-3} + A_{2mk-4}. \quad (41)$$

From these we derive, using (38) the congruences,

$$\left. \begin{aligned} A_{2mk-2} &\equiv A_{2mk} \equiv A'_0 A_{2mk}, \\ A_{2mk-3} &\equiv -a_{k-1} A_{2mk} \equiv -A'_1 A_{2mk}, \\ A_{2mk-4} &\equiv (a_{k-1} a_{k-2} + 1) A_{2mk} \equiv A'_2 A_{2mk}, \\ &\dots\dots\dots \end{aligned} \right\} \pmod{n}.$$

We infer the general law

$$A_{2mk-r} \equiv (-1)^r A'_{r-2} A_{2mk} \pmod{n}. \quad (42)$$

The proof is made by complete induction. We see that the law holds for $r=1$. Suppose it true for all values of r up to and including $r=t$. Then since the continued fractions (1) and (2) are inverse modulo n as far as the partial quotient of order $2mk$ the partial quotient opposite A_{2mk-t} is the same, modulo n , as that opposite A'_t . But we have $A_{2mk-(t+1)} = A_{2mk-(t-1)} - q_{t-1} A_{2mk-t}$, where q_{t-1} is the partial quotient opposite $A_{2mk-(t-1)}$. By means of (42), which by hypothesis holds for $r=t$ this last equation may be written:

$$\begin{aligned} A_{2mk-(t+1)} &\equiv A_{2mk} [A'_{t-3} (-1)^{t-1} - q_{t-1} A'_{t-2} (-1)^t] \\ &\equiv (-1)^{t-1} A_{2mk} (A'_{t-3} + q_{t-1} A'_{t-2}) \equiv (-1)^{t-1} A_{2mk} A'_{t-1}, \end{aligned}$$

which is formula (42) for $r=t+1$. The formula then holds for all values of r . It may also be written

$$A_{2mk-(r+2)} \equiv (-1)^r A_{2mk} A'_r \pmod{n}. \quad (43)$$

Returning with this result to equation (4) we obtain the congruence

$$\begin{aligned} A_{2mk-(kr+1)} &\equiv (-1)^{kr+1} A_{2mk} (-1)^{r-1} A_{kr-1} \pmod{n} \\ &\equiv (-1)^{r(k+1)} A_{2mk} A_{kr-1} \pmod{n}. \end{aligned} \quad (44)$$

Put $r=m$ in this congruence and get $A_{mk-1} \equiv (-1)^{m(k+1)} A_{2mk} A_{mk-1} \pmod{n}$, or

$$A_{mk-1} [A_{2mk} - (-1)^{m(k+1)}] \equiv 0 \pmod{n}. \quad (45)$$

In the same way, starting with equation (5), we get the congruence

$$(-1)^{r(k-1)} A_{2mk} A_{rk} \equiv A_{2mk-rk-2} - M A_{2mk-rk-1} \pmod{n},$$

and putting $r=m$ in this we get $(-1)^{m(k-1)} A_{2mk} A_{mk} \equiv A_{mk-2} - M A_{mk-1}$. But $A_{mk} = mb A_{mk-1} + A_{mk-2}$, whence $(-1)^{m(k-1)} A_{2mk} A_{mk} \equiv A_{mk} - (mb + M) A_{mk-1}$, which we may write in the form

$$A_{mk} [(-1)^{m(k-1)} - A_{2mk}] \equiv (mb + M) A_{mk-1} \pmod{n}. \quad (46)$$

Now by (45) either A_{mk-1} is congruent to zero, or else $A_{2mk} - (-1)^{m(k-1)}$ is congruent to zero, or perhaps both factors are. But if A_{mk-1} is congruent to zero then A_{mk} is not, since, by the equation $A_{mk} B_{mk-1} - A_{mk-1} B_{mk} = (-1)^{mk}$, A_{mk} and A_{mk-1} can have no common factor. Therefore by (46), if A_{mk-1} is congruent to zero, so is $A_{2mk} - (-1)^{m(k-1)}$ also. If, on the other hand, A_{mk-1} is not congruent to zero, then by (45) $A_{2mk} - (-1)^{m(k-1)}$ must be. Therefore we have in all cases,

$$A_{2mk} \equiv (-1)^{m(k-1)} \pmod{n}. \quad (47)$$

V.

Returning to (42) with this last result, we get

$$A_{2mk-r} \equiv (-1)^{r+m(k+1)} A'_{r-2} \pmod{n}. \quad (48)$$

VI.

From the equation $A_{2mk}B_{2mk-1} - A_{2mk-1}B_{2mk} = 1$ we have, using (38) and (47),

$$B_{2mk-1} \equiv (-1)^{m(k-1)} \pmod{n}. \quad (49)$$

VII.

Combining (47) with (44) we obtain

$$A_{2mk-rk+1} \equiv (-1)^{(k+1)(m+r)} A_{rk-1} \pmod{n}. \quad (50)$$

This formula shows that apart from sign the values of A_{rk-1} read backward and forward the same, from $r=0$ to $r=2mk-1$. When k is odd the signs are all the same, while if k is even the signs alternate. It is easily shown that the same theorems apply to the continued fraction (2). Corresponding theorems hold for the denominators B_{rk-1} , but to establish them we must consider continued fraction (17).

VIII.

It will be observed that after the partial quotient y in (17), the succession of partial quotients are the same as in (2). Let us call P_r/Q_r the r -th convergent to the fraction

$$[\overline{a_{k-1}, a_{k-2}, \dots, a_2, a_1, -(b\mu + 2M)}], \quad (\mu = 2, 3, \dots). \quad (51)$$

We have then,

$$A_r'' = A_k'' P_r + A_{k-1}'' Q_r, \quad (52)$$

$$B_r'' = B_k'' P_r + B_{k-1}'' Q_r, \quad (53)$$

$$A_r' = A_k' P_r + A_{k-1}' Q_r, \quad (54)$$

$$B_r' = B_k' P_r + B_{k-1}' Q_r. \quad (55)$$

Solving (52) and (53) for P_r and Q_r we get

$$P_r = (-1)^k (B_{k-1}'' A_r'' - A_{k-1}'' B_r''), \quad (56)$$

$$Q_r = (-1)^k (-B_k'' A_r'' + A_k'' B_r''). \quad (57)$$

Similarly, from (54) and (55),

$$P_r = (-1)^k (B_{k-1}' A_r' - A_{k-1}' B_r'), \quad (58)$$

$$Q_r = (-1)^k (-B_k' A_r' + A_k' B_r'). \quad (59)$$

From (56) and (58) we get

$$B_{k-1}'' A_r'' - A_{k-1}'' B_r'' = B_{k-1}' A_r' - A_{k-1}' B_r', \quad (60)$$

and from (57) and (59) we get

$$-B_k'' A_r'' + A_k'' B_r'' = -B_k' A_r' + A_k' B_r'. \quad (61)$$

Eliminate B_r'' from (60) and (61) and we get

$$B_r' (A_{k-1}'' A_k' - A_{k-1}' A_k'') - A_r' (A_{k-1}'' B_k' - A_k'' B_{k-1}') = (-1)^k A_r''. \quad (62)$$

We proceed to find the values of the quantities in the parentheses. We know from (6) that $A'_{k-1} = A_{k-1}$. Also from (30),

$$A'_k = -[B_{k-1}^2 + A_{k-1}(B_k + B_{k-2}) - (-1)^{k-1}] / A_{k-1};$$

while from (13) $A'_k = -(bA_{k-1} + 2A_{k-2} + B_{k-1})$, and from (25) $A'_{k-1} = B_{k-1}$. Putting these values in the coefficient of B'_r in (62), replacing B_k by its value $bB_{k-1} + B_{k-2}$, and remembering that $A_{k-1}B_{k-2} - A_{k-2}B_{k-1}$ is equal to $(-1)^{k-1}$, we get easily $A'_{k-1}A'_k - A''_kA'_{k-1} = (-1)^{k-1}$. The coefficient of A'_r also reduces. For we have $B'_k = -(b+M)B'_{k-2} + B'_{k-2}$; or, using (8) and (9),

$$B'_k = -(b+M)A_{k-2} + B_{k-2}.$$

Using the same reductions as before, the coefficient of A'_r may be made to take the form $(-1)^{k-1}M$, so that (62) reduces to

$$A'_r = MA'_r - B'_r. \quad (63)$$

If now in this last equation we put $rk-1$ in place of r , and make use of (20) and (50) this may be written:

$$(-1)^r B'_{rk-1} \equiv B_{rk-1} - MA_{rk-1} \pmod{n}. \quad (64)$$

Again, put $r = 2km$ in (63), and note that $A'_{2mk} \equiv (-1)^{m(k+1)} \pmod{n}$, $B'_{2mk-1} \equiv (-1)^{m(k+1)} \pmod{n}$, and by (22) $A''_{2mk} = B'_{2mk} + MB'_{2mk-1}$, and get on reducing,

$$B'_{2mk} \equiv -B'_{2mk} \pmod{n}. \quad (65)$$

IX.

The partial quotient of order $2mk$ in continued fraction (2) is zero, modulo n , so that we may write the following congruences:

$$\left. \begin{aligned} B'_{2mk} &\equiv B'_{2mk-2}, \\ B'_{2mk-1} &\equiv a_1 B'_{2mk-2} + B'_{2mk-3} \equiv (-1)^{m(k+1)}, \\ B'_{2mk-2} &\equiv a_2 B'_{2mk-3} + B'_{2mk-4}, \\ &\dots \end{aligned} \right\} \pmod{n}$$

whence we obtain:

$$\left. \begin{aligned} B'_{2mk} &\equiv B'_{2mk} \equiv -B'_{2mk}, \text{ by (65),} \\ B'_{2mk-1} &\equiv (-1)^{m(k+1)}, \\ B'_{2mk-2} &\equiv -B'_{2mk}, \\ B'_{2mk-3} &\equiv -a_1(-B'_{2mk}) + (-1)^{m(k+1)}, \\ B'_{2mk-4} &\equiv (a_1 a_2 + 1)(-B'_{2mk}) - a_2(-1)^{m(k+1)}, \\ &\dots \end{aligned} \right\} \pmod{n}$$

From these congruences we infer the following which is easily established by complete induction

$$B'_{2mk-r} \equiv (-1)^r (-A_{r-2} B'_{2mk} - (-1)^{m(k+1)} B'_{r-2}) \pmod{n}. \quad (66)$$

Put $r=2mk-1$ in this last congruence and get

$$B'_1 \equiv A_{2mk-3} B_{2mk} + (-1)^{m(k+1)} B_{2mk-3} \pmod{n}. \quad (67)$$

But $B'_1=1$ and $A_{2mk-1}-a_{k-1}A_{2mk-2}=A_{2mk-3}$, $B_{2mk-1}-a_{k-1}B_{2mk-2}=B_{2mk-3}$, so that $A_{2mk-3} \equiv a_{k-1}(-1)^{m(k+1)} \pmod{n}$, and (67) reduces easily to

$$B_{2mk} \equiv -B_{2mk-2} \pmod{n}. \quad (68)$$

But since the partial quotient of (1) of rank $2mk$ is $-2M$, and $B_{2mk-1} \equiv (-1)^{mk+1}$, we have $B_{2mk} \equiv -2M(-1)^{mk+1} + B_{2mk-2} \pmod{n}$, so that, by (68),

$$B_{2mk} \equiv -M(-1)^{mk+1} \pmod{n}. \quad (69)$$

Returning with this value to (66) we get

$$B'_{2mk-r} \equiv (-1)^{m(k+1)+r+1} (B_{r-2} - MA_{r-2}) \pmod{n}. \quad (70)$$

X.

Reading backward from B_{2mk} , as in the derivation of (66) we arrive at the formula

$$B_{2mk-r} \equiv (-1)^{m(k+1)+r+1} (B'_{r-2} - MA'_{r-2}) \pmod{n}. \quad (71)$$

In this formula put $r=tk+1$; then

$$B_{2mk-tk-1} \equiv (-1)^{m(k+1)+tk} (B'_{tk-1} - MA'_{tk-1}) \pmod{n}, \quad (72)$$

and this with (63) gives $B_{2mk-tk-1} \equiv (-1)^{m(k+1)+tk-1} A''_{tk-1} \pmod{n}$. But, by (20) this gives

$$B_{2mk-tk-1} \equiv (-1)^{(m+t)(k+1)} B_{tk-1} \pmod{n}, \quad (73)$$

which is the same relation between the B 's as (50) between the A 's.

XI.

From (72) and (73) we get easily

$$B_{tk-1} \equiv (-1)^t (B'_{tk-1} - MA'_{tk-1}) \pmod{n}, \quad (74)$$

while (71) gives the corresponding formula:

$$B'_{tk-1} \equiv (-1)^t (B_{tk-1} - MA_{tk-1}) \pmod{n}. \quad (75)$$

XII.

Let m' now be the odd value of μ less than $2n$ which satisfies the congruence, $\mu b + 2M \equiv 0 \pmod{n}$, and suppose first $2m$ is greater than this odd value so that $2m-m'=n$. We have

$$A_{2mk-1} \equiv 0 \equiv A_{nk} A_{m'k-1} + A_{nk-1} B_{m'k-1} \pmod{n}, \quad (76)$$

$$A_{2mk} \equiv (-1)^{m(k+1)} \equiv A_{nk} A_{m'k} + A_{nk-1} B_{m'k} \pmod{n}. \quad (77)$$

Eliminate A_{nk-1} from these two equations and get

$$B_{m'k-1} \equiv A_{nk} (-1)^{k(m-m')+m} \pmod{n}. \quad (78)$$

But by (50) and (73) we know that

$$A_{nk-1} = (-1)^{(k+1)(m'+m)} A_{m'k-1} \pmod{n}, \quad (79)$$

$$B_{nk-1} \equiv (-1)^{(k+1)(m'+m)} B_{m'k-1} \pmod{n}, \quad (80)$$

so that

$$A_{nk} \equiv -B_{nk-1} \pmod{n}. \quad (81)$$

But $A_{2nk-1} = A_{nk}A_{nk-1} + B_{nk-1}A_{nk-1} = A_{nk-1}(A_{nk} + B_{nk-1})$, so that by (81) we have

$$A_{2nk-1} \equiv 0 \pmod{n}. \quad (82)$$

Also $B_{2nk} = A_{nk}B_{nk} + B_{nk}B_{nk-1}$; and this by (81) gives

$$B_{2nk} \equiv 0 \pmod{n}. \quad (83)$$

Again, $A_{2nk} = A_{nk}A_{nk} + A_{nk-1}B_{nk} \equiv -A_{nk}B_{nk-1} + A_{nk-1}B_{nk}$, by (81), and by (82) and (83) this gives

$$A_{2nk} \equiv (-1)^{nk-1} \pmod{n}. \quad (84)$$

And, finally, from the equation $A_{2nk}B_{2nk-1} - A_{2nk-1}B_{2nk} = 1$, we derive

$$B_{2nk-1} \equiv (-1)^{nk-1} \pmod{n}. \quad (85)$$

XIII.

Suppose next that m' is greater than $2m$ so that $m' - 2m = n$. We have then

$$A_{m'k} \equiv A_{nk}A_{2mk} + A_{nk-1}B_{2mk}, \quad A_{m'k-1} \equiv A_{nk}A_{2mk-1} + A_{nk-1}B_{2mk-1}.$$

Put in these the values of A_{2mk} , etc., already derived, and these equations become

$$(-1)^{mk+1} A_{m'k} \equiv A_{nk} - MA_{nk-1} \pmod{n}. \quad (86)$$

$$(-1)^{mk+1} A_{m'k-1} \equiv A_{nk-1} \pmod{n}. \quad (87)$$

$$(-1)^{mk+1} B_{m'k} \equiv B_{nk} - MB_{nk-1} \pmod{n}. \quad (88)$$

$$(-1)^{mk+1} B_{m'k-1} \equiv B_{nk-1} \pmod{n}. \quad (89)$$

From these we get

$$A_{nk} + B_{nk-1} \equiv (-1)^{mk+1} (A_{mk} + MA_{mk-1} + B_{mk-1}). \quad (90)$$

But, recalling the definition of m' we observe that the fractions (1) and (2), as far as the $km' - 1$ -st term, are inverse modulo n , so that

$$A_{m'k-1} \equiv A'_{m'k-1} \pmod{n}. \quad (91)$$

$$A_{m'k-2} \equiv B'_{m'k-1} \pmod{n}. \quad (92)$$

$$B_{m'k-1} \equiv A'_{m'k-2} \pmod{n}. \quad (93)$$

$$B_{m'k-2} \equiv B'_{m'k-2} \pmod{n}. \quad (94)$$

Also by (5), since m' is odd, $-A_{m'k} = A_{m'k} + MA_{m'k-1}$.

Further, since the $m'k$ -th partial quotient is zero in (2),

$$A_{mk} \equiv A_{mk-2} \pmod{n}, \quad (95)$$

whence, from (92) and (95)

$$A_{mk} + MA_{mk-1} \equiv -B_{mk-1} \pmod{n}, \quad (96)$$

which in (90) gives $A_{nk} + B_{nk-1} \equiv 0 \pmod{n}$, and this is the same formula as (81) for the case where $2m$ is greater than m' . Formulae (82), (83), (84) and (85) therefore hold whether $2m$ is greater or less than m' .

XIV.

From the equations

$$A_{4nk} = A_{2nk} + A_{2nk-1}B_{2nk}, \quad (97)$$

$$A_{4nk-1} = A_{2nk}A_{2nk-1} + A_{2nk-1}B_{2nk}, \quad (98)$$

$$B_{4nk} = B_{2nk}A_{2nk} + B_{2nk-1}B_{2nk}, \quad (99)$$

$$B_{4nk-1} = B_{2nk}A_{2nk-1} + B_{2nk-1}B_{2nk-1}, \quad (100)$$

we now derive

$$A_{4nk} \equiv B_{4nk-1} \equiv 1 \pmod{n}, \quad (101)$$

$$A_{4nk-1} \equiv B_{4nk} \equiv 0 \pmod{n}. \quad (102)$$

From these results it appears that taken modulo n the series of convergents repeat themselves with a period of $4nk$, but if k is odd as well as n , the period is $2nk$.

XV.

We now extend the above results to the fraction

$$(\overline{a_1, a_2, a_3, \dots, a_{k-1}, \mu b + c}), \quad (\mu = 1, 2, 3, \dots), \quad (103)$$

where, as before, n is prime to $2b$, and to A_{k-1} and B_{k-1} . It is clear that there will be a partial quotient $\mu b + c \equiv 0 \pmod{n}$, after which the fraction is of the type (1). Call P_r/Q_r the r -th convergent of (103) and as before A_r/B_r the r -th convergent of (1). Then we have, μ being determined by the congruence $\mu b + c \equiv 0 \pmod{n}$,

$$P_{\mu+2nk-1} \equiv P_{\mu k}A_{2nk-1} + P_{\mu k-1}B_{2nk-1} \pmod{n}. \quad (104)$$

$$P_{\mu+2nk} \equiv P_{\mu k}A_{2nk} + P_{\mu k-1}B_{2nk} \pmod{n}. \quad (105)$$

$$Q_{\mu+2nk-1} \equiv Q_{\mu k}A_{2nk-1} + Q_{\mu k-1}B_{2nk-1} \pmod{n}. \quad (106)$$

$$Q_{\mu+2nk} \equiv Q_{\mu k}A_{2nk} + Q_{\mu k-1}B_{2nk} \pmod{n}. \quad (107)$$

But we have also,

$$P_{\mu+2nk-1} \equiv P_{2nk}P_{\mu k-1} + P_{2nk-1}Q_{\mu k-1} \pmod{n}. \quad (108)$$

$$P_{\mu+2nk} \equiv P_{2nk}P_{\mu k} + P_{2nk-1}Q_{\mu k} \pmod{n}. \quad (109)$$

$$Q_{\mu+2nk-1} \equiv Q_{2nk}P_{\mu k-1} + Q_{2nk-1}Q_{\mu k-1} \pmod{n}. \quad (110)$$

$$Q_{\mu+2nk} \equiv Q_{2nk}P_{\mu k} + Q_{2nk-1}Q_{\mu k} \pmod{n}. \quad (111)$$

Using (82), (83), (84) and (85), we derive from these,

$$P_{\mu k-1} [(-1)^{nk-1} - P_{2nk}] \equiv P_{2nk-1}Q_{\mu k-1} \pmod{n}. \quad (112)$$

$$P_{\mu k} [(-1)^{nk-1} - P_{2nk}] \equiv P_{2nk-1}Q_{\mu k} \pmod{n}. \quad (113)$$

$$Q_{\mu k-1} [(-1)^{nk-1} - Q_{2nk-1}] \equiv Q_{2nk}P_{\mu k-1} \pmod{n}. \quad (114)$$

$$Q_{\mu k} [(-1)^{nk-1} - Q_{2nk-1}] \equiv Q_{2nk}P_{\mu k} \pmod{n}. \quad (115)$$

Eliminate now P_{2nk-1} from (112) and (113) and obtain

$$(P_{\mu k-1}Q_{\mu k}-P_{\mu k}P_{\mu k-1})[(-1)^{nk-1}-P_{2nk}]\equiv 0 \pmod{n}.$$

Then, since the first factor on the left is ± 1 , we have

$$P_{2nk}\equiv (-1)^{nk-1} \pmod{n}. \quad (116)$$

Similarly, from (114) and (115) we get,

$$Q_{2nk-1}\equiv (-1)^{nk-1} \pmod{n}. \quad (117)$$

Also, by (112) and (113), $P_{2nk-1}Q_{\mu k-1}\equiv 0 \pmod{n}$, $P_{2nk-1}Q_{\mu k}\equiv 0 \pmod{n}$, and since $Q_{\mu k}$ and $Q_{\mu k-1}$ can not both be congruent to zero on account of the equation $P_{\mu k}Q_{\mu k-1}-P_{\mu k-1}Q_{\mu k}=(-1)^{\mu k}$, we must have

$$P_{2nk-1}\equiv 0 \pmod{n}, \quad (118)$$

and, similarly,

$$Q_{2nk}\equiv 0 \pmod{n}. \quad (119)$$

XVI.

The above results may be extended to fractions which have a set of "irregular" or non-periodic partial quotients followed by partial quotients of the sort considered in fraction (103). Such a fraction would be of the form

$$(q_1, q_2, \dots, q_r, \overline{a_1, a_2, \dots, a_{k-1}, \mu b + c}), \quad (\mu=1, 2, 3, \dots).$$

For this fraction there will be r non-periodic convergents, after which the periodicity begins, the length of the period being the same as for the fraction (103). The two successive convergents which close each period will, however, not be congruent respectively to $\pm 1, 0$ and $0, \pm 1$, but to the $(r-1)$ -st and the r -th convergents respectively of the fraction $(q_1, q_2, \dots, q_r)$.

XVII.

We consider now the special cases which have been ruled out in the statement of our theorems, and take up first the case where b is congruent to zero, modulo n . This will include also the case where b is actually zero, in which case the fraction is an ordinary purely periodic continued fraction. We may write it in the form $\overline{(a_1, a_2, a_3, \dots, a_k)}$. The convergents of order k and $k-1$ are connected with those of order $2k$ and $2k-1$ by the following equations:

$$\begin{aligned} A_{2k} &= A_k^2 + A_{k-1}B_k, & B_{2k} &= B_kA_k + B_{k-1}B_k, \\ A_{2k-1} &= A_kA_{k-1} + A_{k-1}B_{k-1}, & B_{2k-1} &= B_kA_{k-1} + B_{k-1}^2. \end{aligned}$$

Now, these are seen to result from the same process as that by which two linear homogeneous substitutions are compounded, so that if we call T_k the substitution,

$$T_k = \begin{pmatrix} A_k & B_k \\ A_{k-1} & B_{k-1} \end{pmatrix},$$

we have $T_{2k} = T_k^2$, and in general, $T_{rk} = T_k^r$. Now the theory of the periodicity of such a substitution modulo a prime is well known. Gierster has shown (*Math. Ann.*, Vol. XVIII, p. 322) that the period with respect to a prime modulus p of $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, where $\alpha\delta - \beta\gamma \equiv 1 \pmod{p}$, depends upon the quadratic character of $\Delta = (\alpha + \delta)^2/4 - 1$ with respect to p . In fact, if we denote the quadratic character by ϵ , where ϵ is $+1$ if Δ is a quadratic residue of p ; -1 if Δ is a quadratic non-residue of p , and 0 if Δ is divisible by p , then the period of $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ is a divisor of $p - \epsilon$. More narrowly, the period is a divisor of $(p - \epsilon)/2$ if p is not a divisor of Δ , and the period is p if p is a divisor of Δ . In Gierster's discussion the period would be considered closed when some power of the substitution should be of the form $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$, since in that case the x could be divided out of the fractional substitution. Manifestly in the application of his results to our problem no such division is possible. Using Gierster's results we may state the following theorem:

The purely periodic continued fraction $\overline{(a_1, a_2, \dots, a_k)}$ taken with respect to a prime, modulus p , recurs with a period $\delta\pi k$ where δ is some divisor of $p - \epsilon$, where $\epsilon = \pm 1$ or zero according as $\Delta = (A_k + B_{k-1})^2/4 - (-1)^k$ is a quadratic residue, a quadratic non-residue, or a divisor of p , while π is the exponent to which $A_{k\delta}$ belongs, modulo p .

XVIII.

In congruence (37) we have restricted n to be prime to $2b$. For odd values of n all of our results are still valid if n and $2b$ are not relatively prime, provided that the congruence (37) has roots; that is, provided the greatest common divisor of n and b also divides $2M'$ where M' is an integer congruent modulo m to the fraction M . (The existence of such an integer M' follows from the fact that we are still supposing n to be prime to the denominator A_{k-1} of M). If the congruence (37) does not have roots the discussion given above does not apply, and the intrinsic importance of congruence (37) in the theory appears when we observe that if it has no roots the general results which we have obtained no longer hold, as the numerical example $\overline{(3, 2, 1, 4, 7m)} \pmod{21}$ shows. If the congruence (37) has no roots we compute the period of the partial quotients and apply the less definite method of the preceding paragraph.

For even values of n the further difficulty arises in that while (37) may have roots, the values of the unknown will all be even, or all odd, so that the results of XII and XIII do not apply. By an analysis similar to that used in XII we may show, however, that formulae (82), (83), (84) and (85) hold for this case also. They do not hold if (37) has no roots.

XIX.

In the case where A_{k-1} is congruent to zero, modulo n , the congruence (37) becomes meaningless by the definition of M . The sequence of A 's is, however, easily determined. For from the equation, $A_{k+r} = A_k A_r + A_{k-1} B_r$, we get, $A_{k+r} \equiv A_k A_r \pmod{n}$, so that the list of A 's from A_{k+1} to A_{2k} is obtained by multiplying the list from A_1 to A_k by A_k , and so on. In particular, the list of values of A_{rk-1} , ($r=1, 2, 3, \dots$) are all zero, while $A_{rk} \equiv A_k^r \pmod{n}$, from which, by Fermat's Theorem, $A_{2nk} \equiv A_k^{2n} \equiv A_k^2 \pmod{n}$. From this congruence it is clear that unless A_k belongs to the exponent 2, modulo n , the period of the convergents can not close with the one of order $2nk$. If g is the exponent to which A_k belongs, modulo n , then the period of the convergents must be a multiple of gnk .

XX.

In conclusion we apply the foregoing results to establish the theorems mentioned in the introduction which relate to the continued fraction for $e = (2, 1, 2, 1, 1, 4, 1, 1, 6, \dots)$. The convergents to this fraction are connected with those of the fraction $e-1 = (1, 1, 2, 1, 1, 4, \dots)$ by the simple equations, easily established, $A_m - B_m = A'_m$, $B_m = B'_m$, where the convergent A/B refers to the first fraction and A'/B' to the second. Now for the second fraction the value of M is found to be unity, so that congruence (37) becomes $2\mu + 2 \equiv 0 \pmod{n}$. Suppose first that n is odd. The congruence has the root $\mu \equiv -1$, so the two values of μ less than $2n$ which satisfy this congruence are $n-1$ and $2n-1$, of which the first is even. Put this for $2m$ in (38), (47), (49) and (69), and remember that $k=3$ in this fraction and get

$$\begin{aligned} A'_{3n-4} &\equiv 0 \pmod{n}, & B'_{3n-4} &\equiv 1 \pmod{n}, \\ A'_{3n-3} &\equiv 1 \pmod{n}, & B'_{3n-3} &\equiv -1 \pmod{n}. \end{aligned}$$

From these, knowing that $a_{3n-2} = 1$ and $a_{3n-4} = 1$ and $a_{3n} \equiv 0 \pmod{n}$, we readily compute

$$\begin{aligned} A'_{3n} &\equiv 1 \pmod{n}, & B'_{3n} &\equiv 0 \pmod{n}, \\ A'_{3n-1} &\equiv 2 \pmod{n}, & B'_{3n-1} &\equiv -1 \pmod{n}, \end{aligned}$$

whence

$$\begin{aligned} A_{3n} &\equiv 1 \pmod{n}, & B_{3n} &\equiv 0 \pmod{n}, \\ A_{3n-1} &\equiv 1 \pmod{n}, & B_{3n-1} &\equiv -1 \pmod{n}. \end{aligned}$$

From these follow the rest of the results mentioned. The results for even values of n are easily obtained.